

INFORMATION TECHNOLOGY DEPARTMENT

–SECURITY DIVISION–

Avoid phishing scams with three simple steps



1

Check the email address & sender name

Look carefully at the email address. It may have extra words, letters, numbers or strange spelling. Scammers use familiar names or pretend to be someone you know.

2

Look for poor grammar & urgency

Awkward writing and grammar errors, as well as pressure (urgency) to act now or something bad will happen, are both warning signs of a scam.

3

Check for suspicious attachments or links

Scammers will prompt you to click a link or verify your password in order to steal your information or lock you out of your computer.

To check a suspicious link, hover your mouse over it – but DO NOT CLICK.

How to Report an Incident

- **Submit an IT Helpdesk Support Ticket**
 - <https://sbcusd.gethelpss.com/>
- **Contact the IT Help Desk**
 - 909-888-4357
 - Monday-Friday 7:30am-4:00pm



To learn more

Visit the IT web resource page at:
www.sbcusd.com/thinksecure